Title (en)

Stream ciphering of the content of a memory which is external to a processor

Title (de)

Stromverschlüsselung des Inhalts eines Speichers, welcher ausserhalb eines Prozessors angeordnet ist

Title (fr)

Chiffrement en continu du contenu d'une mémoire externe à un processeur

Publication

EP 1617586 A1 20060118 (FR)

Application

EP 05106111 A 20050705

Priority

FR 0451459 A 20040706

Abstract (en)

The method involves applying a ciphering algorithm with a function of a key specific to an integrated circuit of an initialization vector. A ciphered data is memorized, where the initialization vector includes a storage address of the data in a memory and a differentiation value. An algorithm identical to the ciphering algorithm is applied based on the address of the ciphered data. An independent claim is also included for a smart card comprising an electronic assembly.

IPC 8 full level

H04L 9/18 (2006.01); **G06F 12/14** (2006.01); **G06F 21/00** (2006.01)

CPC (source: EP US)

G06F 12/1408 (2013.01 - EP US); **H04L 9/065** (2013.01 - EP US); H04L 2209/12 (2013.01 - EP US)

Citation (search report)
- [Y] EP 0908810 A2 19990414 - GEN INSTRUMENT CORP [US]
- [Y] US 2002044651 A1 20020418 - TUVELL WALTER E [US]
- [Y] GB 2353191 A 20010214 - HW COMM LTD [GB], et al
- [DA] US 2003198344 A1 20031023 - COURCAMBECK STEPHAN [FR], et al

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

DOCDB simple family (publication)

EP 1617586 A1 20060118; **EP 1617586 B1 20080903**; AT E407494 T1 20080915; DE 602005009439 D1 20081016; US 2006008079 A1 20060112; US 8045712 B2 20111025

DOCDB simple family (application)

EP 05106111 A 20050705; AT 05106111 T 20050705; DE 602005009439 T 20050705; US 17591505 A 20050706